Development of the Application for Diploma Authenticity Using the Blockchain Technology

Kseniia Nikolskaia[1], Daria Snegireva
South Ural State University
Chelyabinsk, Russia
1nikolskaya174@gmail.com

Aleksey Minbaleev
Department of Information Law and Digital Technologies
Kutafin Moscow State Law University
Moscow, Russia
alexmin@bk.ru

***Abstract*—Global digitalization of society implies the availability of information, as well as verification of its authenticity from anywhere in the world. Providing digital diplomas. the analogue of paper ones, is an actual task. In the current paper the step-by-step development of an application for authentication of diplomas using blockchain technology is considered. Also the concept, structures and operation mechanism of the blockchain are described.**

Keywords— digital diploma; blockchain technology; digital economy

I. INTRODUCTION

One of the urgent problems of digital education is students' certification and particularly giving them the digital academic diplomas. The solution of such issue would increase the openness and transparency in issuance of educational diplomas and reduce the possibility of falsification and fakes. At the same time, potential employers could instantly identify and verify diplomas of applicants for vacant positions allowing graduates of educational institutions to confirm the status of their diplomas at any time [1]. As long as a block in a chain is difficult to fake, the blockchain technology provides a safe transparent environment for storing documents about education owing to the use of a chain of blocks for recording information. In this case the employer can be confident in the authenticity of the applicant's documents. The second part of the article deals with the related assignments. The third part describes the concept, structure and mechanism of the blockchain. The fourth part describes the Blockcerts platform. In the fifth part the step-by-step implementation of the project is presented. The sixth part describes the operation of the web service. The seventh part includes the conclusion and further areas of work. The whole project code including all comments and configuration files is located at: https://github.com/DasHaSneg/Checkblockchaindiplomas.

II. RELATED WORK

Nowadays, there are few universities that have begun the implementation systems for issuing diplomas which are based on blockchain technology.

A. Checking Diplomas of Financial University (подробнее какой университет) in terms of the blockchain system

The Financial University implemented the blockchain authentication of diplomas on its official website in 2018 [2]. The every individual entry is signed by the university. This is a protection against the recording for third parties. Such counterfeits will not be verified and therefore will not be recognized as valid. The data is encrypted using the SHA-256 algorithm [3] As a result, the unique identifier is obtained for each diploma - the diploma hash. The downside is that the hash function of the diploma can not be entered into the input form. The system does not use one of the main advantages of storing a diploma in a blockchain - the ability for a student to store one small hash function instead of the full version of the document.

B. MIT Degree Verification

MIT Degree Verification is a certificate verification site where any individual can conduct an independent diploma verification. Employers can check the diploma by inserting a link or downloading a file with digital diploma of the student and then immediately receive a response from the portal [4]. The system uses the blockchain as a notary, it finds the transaction identifier in the document, checks the keys and confirms that nothing has been changed.

III. CONCEPT, STRUCTURE AND BLOCKCHAIN WORK PRINCIPLES

The blockchain is a distributed database with the storage devices which are not connected to a common server. This database stores an ever-growing list of ordered records called blocks. Each block contains a timestamp and a link to the previous block [5].

There are three types of blockchain: public, private and consortium blockchain.

A. Public blockchain

The public blockchain is available for anyone in the world [6]. It means that they can send transactions and wait for them to turn on if they are valid as well as participate in the consensus process, particularly in determining which blocks are added to the chain. The advantages of the public blockchain are that each transaction is publicly available, and users can be anonymous. However, the disadvantages are the fairly slow working process and significant expenses of energy and

978-1-7281-2595-4/19/$31.00 ©2019 IEEE

memory because the necessity in synchronization with the entire chain of blocks starting with the genesis of the block.

B. Private blockchain

Fully private blockchain is a chain of blocks in which the recording of new blocks is assigned to only one organization. Permission to read may be publicly available or limited. The advantage is that transactions in a private block chain are performing much faster than in a public blockchain. The downside of the private blockchain is that it does not offer the same decentralized security as its public equivalent.

C. Consortium blockchain

Consortium blockchain are controlled by a pre-selected set of nodes. Vitaly Buterin cites as an example a system of 15 financial institutions each of which controls the node, 10 of which must confirm each block in order to be recognized as valid and added to the chain. The right to read a block chain can be publicly available or limited to participants. The "Hybrid" systems are possible whether the root-hashes of the blocks are publicly available, although the all blockchain members can make solely a limited number of requests and transaction confirmations of certain parts of the blockchain. Such chains can be called "partially decentralized." The consortium blockchain has the same advantages as a private blockchain but it does not work under a single but the leadership of a group.

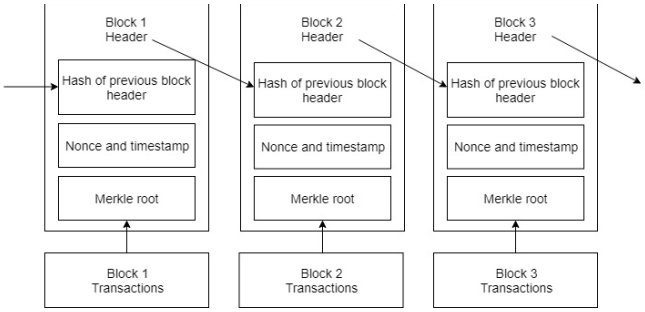

Fig. 1. Blockchain structure

The blockchain has a common structure, no matter of its type. It is often visualized as a vertical stack with blocks located one above the other where the very first block serves as the basis of the stack. Each block in the chain is identified by a hash generated using the SHA256 cryptographic hash algorithm [7] in the block header. Each block refers to the previous block, known as the parent block, through the previous block hash field in the block header. In other words, each block contains the hash of its parent within its own header. The sequence of hashes connecting each block to its parent creates a chain that returns completely to the first block ever created, known as the genesis block. The block is a container that combines transactions for inclusion in the public registry - the blockchain. The block consists of a header containing metadata and the body from the list of transactions. The block header consists of three sets of metadata. The first part of the metadata is a link to the previous block hash that connects this block to the previous block in the blockchain. The second is a set of metadata, a time stamp and some random number filled with miners. The third part is the root of the Merkle tree - a data structure used to effectively summarize all transactions in the block.

The Merkle tree, known as a binary hash tree, is a data structure used to efficiently summarize and verify the integrity of large data sets. Merkle trees are binary trees containing cryptographic hashes. The term "tree" is used in computer science to describe the structure of branching data but these trees are usually displayed upside down with the "root" at the top and the "leaves" at the bottom of a diagram. Merkle trees are used in the blockchain to summarize all transactions in the block creating a common digital fingerprint of the entire set of transactions and providing a very efficient process for checking whether a transaction is included in the block. The Merkle tree is being created by recursively hashing pairs of nodes until there is only one hash called the "root".

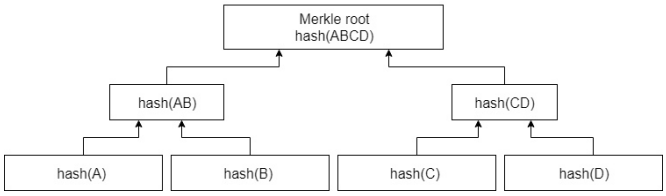

Fig. 2. Merkle tree

Despite the fact that the blockchain is a distributed system, each node can form transactions. This does not mean that all participants of the blockchain network have equal rights - in almost any implementation of this technology, roles are assigned to miners (participants writing transactions to the journal), auditors and light clients. Moreover, such a division is valid not only for private blockchains but also for open blockchains. For instance, Bitcoin [8]. The light clients do not have the full version of the blockchain and contain only important data for the site. For this reason, they are the good option for organizing a cryptocurrency wallet - such client will not give the whole picture of the network but allows to effectively track the user's balance. The light clients require less computational resources and memory, so they can work on mobile platforms. The second type is when the audit nodes do not participate in the consensus process but they have a full copy of the blockchain. The "Auditors" regularly check the work of miners and distribute the load across the network performing the function of a kind of content delivery network (CDN) for the blockchain data. The third type is the miners or the knots of consensus. They are rewarded for their work (mining) by generating new portions of cryptocurrency. The miners are actively involved in the formation of the blockchain constantly grouping incoming transactions into blocks and distributing them throughout the network. The process of searching for blocks is called mining [9].

The miner must solve a really difficult computational puzzle in a relatively short period of time. This mechanism, known as consensus, was created to ensure that no one had monopoly power over the ability to write to a journal and thus could not manipulate its content or censor the information included in it [10]. For example, Bitcoin uses the algorithm of consensus Proof of Work [11].

The purpose of the consensus algorithm is to make it possible to safely update the state according to certain rules of

state transition where the right to make state changes is distributed between a certain economic set. The task of this mechanism (algorithm) is to correctly record information in the blockchain as well as to ensure the safe and efficient operation of the cryptocurrency network.

When several new blocks are simultaneously formed the chain branching can frequently occur, each of them has the same block as the parent. The branch stops as soon as a new block is found which carries on any of the branches. All nodes switch to the circuit that has the longest version and then continue to work on its extension [12].

Transactions are broadcasting to the entire network by the sender — the nodes collect information and include them in the found block which are based on certain conditions [13].

The miner gathers together the new received entries from other network participants, then forms the title of the future block and calculates the block key. To find a suitable key value miners have to do a huge amount of recalculations. When a suitable key is found the miner saves the block and sends it to other members of the network. Thus all entries in the block are confirmed and protected by a key that is very difficult to fake. Moreover, the key of the previous block is coded in the block key as well which now cannot be forged. This sophisticated key calculation procedure complicates the creation of a block. Furthermore, it complicates the creation of fake blocks making that almost impossible [14].

The time of generation of a managed block is achieved by adding the complexity value inside the block. In terms of the Bitcoin blockchain, the block hash should be strictly less than the specified value which should be accepted. This value varies depending on the total computing power of the network. The more powerful the network is the smaller the set value is and consequently the more difficult it is to create a block [15].

The complexity of the task is regulated by the network so that there would be found a certain number of blocks — it is six blocks per hour for Bitcoin (one block per ten minutes).

IV. PPLATFORM FOR IMPLEMENTING BLOCKCERTS

There are several platforms for the implementation of such systems. We settled on the Blockcerts system. The Blockcerts consists of open source libraries, tools and mobile applications. The Blockcerts contains components for creating, issuing, viewing and verifying certificates in any blockchain [16]. Issuing a certificate presented on is relatively simple: a digital file is created which contains basic information such as the recipient's name, publisher's name (university name), release date, etc. The certificate is then signed using the private key which only the publisher has the access to. Next, the hash function is created which can be used to verify that the certificate has not been changed. Finally, the private key is used again to create an entry in the blockchain which states that this certificate was issued to a specific person on a particular day. The system allows you to check who was issued a certificate and its content.

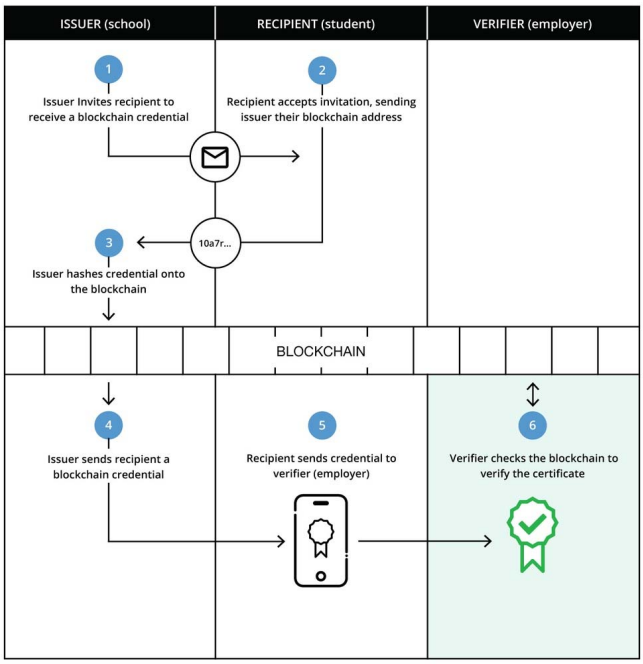

Fig. 3. Blockcerts work pattern

The Blockcerts use a batch issue diplomas because it is much more efficient to use one transaction to issue several certificates at once. The publisher creates the Merkle tree of diplomas and registers the Merkle root as the OP_RETURN [10] field in a Bitcoin transaction.

The Certificates of the Blockcert system consist of the diploma itself and a receipt which contains:

1. The bitcoin transaction identifier storing the Merkle root.

2. The expected Merkle root on the blockchain.

3. The expected hash for the i-th diploma of the recipient.

4. The path of Merkle from the i-th recipient's certificate to the root of the Merkle.

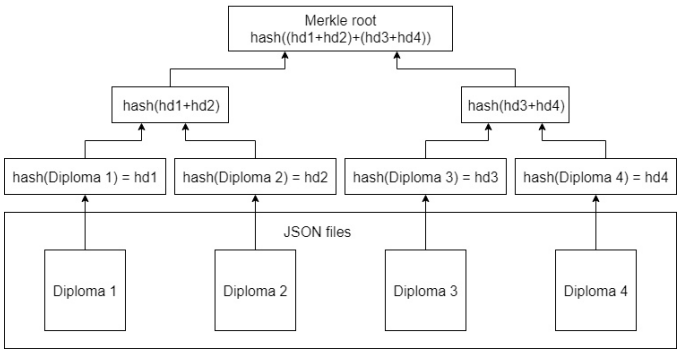

Fig. 4. Merkle Tree of Diplomas

The Blockcerts scheme extends the OpenBadges [9] scheme using the JSON-LD context [6].

It is hashed and is the diploma of the contents of the JSON certificate without signature. What comes after signature is the receipt which the hashed diploma is compared with during the verification.

Certificate verification consists of several stages:

1. The diploma is not forged.

Diploma authentication consists of three steps.

1.1. Verification of evidence Merkle.

1.2. Comparison the local diploma's hash with the value in the receipt.

1.3. Comparison of the Merkle root in the diploma with the value in the blockchain transaction.

2. The term of the diploma has not expired.

The diploma may contain an expiration date. If it exists the test should compare the expires field value with the current time.

3. The diploma is not withdrawn by the publisher.

The diploma field indicates where to get the list of revoked publisher diplomas. Open Badges compatible the Blockcerts use HTTP URI [16] according to the Open Badges specification.

According to Open Badges, for the Blockcerts the diploma is considered revoked if any id entry in the revokedAssertions array contains the diploma identifier. The diploma identifier is available in the id field.

If a diploma has been recalled, (optional) revocationReason can provide additional information about the reasons in revocationReason.

4. Authentication of the publisher.

In the badge.issuer.id field of the blockchain diploma there is information about the location of valid keys' records.

We get a timestamp and an input address from the blockchain transaction information. For example, regarding Blockchain.info [17] we need the addr field from the inputs of the array and the time field. The time stamp and the input address from the details of the blockchain transaction are used. The timestamp and address must match [18].

V. Realization

A. Creating a diploma template

A console command from the cert-tools Blockcerts command line tools was used to create an unsigned diploma template and the unsigned diplomas as well.

B. Publication of diplomas in the blockchain

To publish the diplomas in the blockchain the commander tools of the cert-issuer from Blockcerts were used and the bitcoin testnet was chosen as the blockchain.

C. Obtaining Bitcoin Testnet's public address

To create an address use the bitcoin core testnet console. The first argument is a label, if specified, it is added to the address book. Thereby, the payments that are received at the address are associated with the "label".

D. Obtaining test coins

Test coins have no real value, so you can get them by specifying your public address.

To obtain test coins the site Mempool was used. To obtain test coins you must enter the solution of the arithmetic example of the image, the public address and the desired number of test coins. After using they must be returned to the address which is indicated by the creator of the site.

Fig. 5. Website for receiving test coins

The Fig. 12 depicts the transaction. In order to let the test coins become available you need to wait for confirmation.

Fig. 6. Transaction with receipt of test coins

E. Publication of diplomas in blockchain

Listing 1. The command for publishing diplomas on the blockchain

```
instantiate-certificate-batch -c conf.ini
```

This command requires a configuration file (option –c).

Listing 2. Listing the configuration file myconf.ini

```
issuing_address                                =
muf6mqLy1sGPCEmMyFHsYvZDXHLSarfwao
unsigned_certificates_dir=C:\cert-
issuer2\cert-issuer\data\unsigned_certifi
cates
blockchain_certificates_dir=C:\cert-
issuer2\cert-issuer\data\blockchain_ce
rtificates
```

```
key_file = pk_issuer.txt
chain=bitcoin_testnet
no_safe_mode
```

F. *Diploma authentication*

To verify the authenticity of the diploma the cert-verifier library was used.

Listing 3. Check diploma in blockchain

```
certificate = cert_store.get_certificate(certificate_uid)
    if certificate:

options={'etherscan_api_token':''}
        verify_response = verifier.verify_certificate(certificate, options=options)
        return verify_response
    else:
          raise Exception('Cannot find certificate with uid=%s', certificate_uid)
```

VI. WWeb Service Development

The principle of the web service operation is shown in the sequence diagram/

In order to launch the verification of the diploma the user loads the file with it, the file name is displayed. To check the diploma the user clicks the "Check" button. The diploma is saved to the hard disk and processed. The processed information about the diploma is displayed to the user. A diploma check is requested. The verification and result steps are displayed to the user.

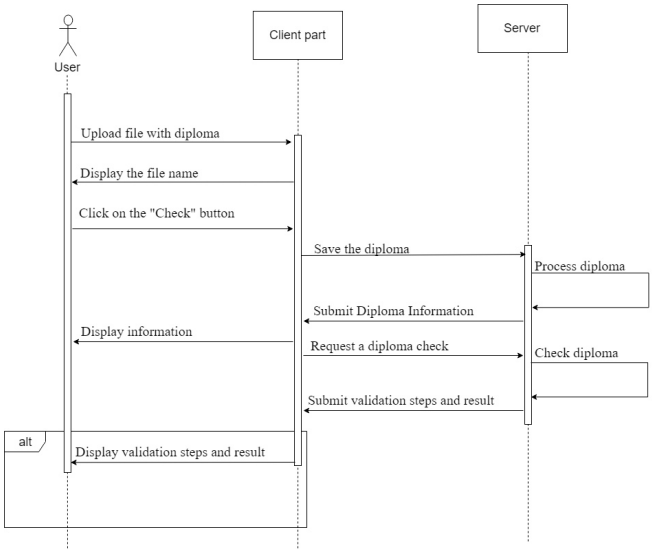

Fig. 7. Sequence diagram

To make the process of checking diplomas convenient the web service was developed.

HTML5 and CSS3 templates were drawn and stacked for the web service. The javascript language was used to add interactivity. The result is shown in Fig. 9.

Fig. 8. Download page

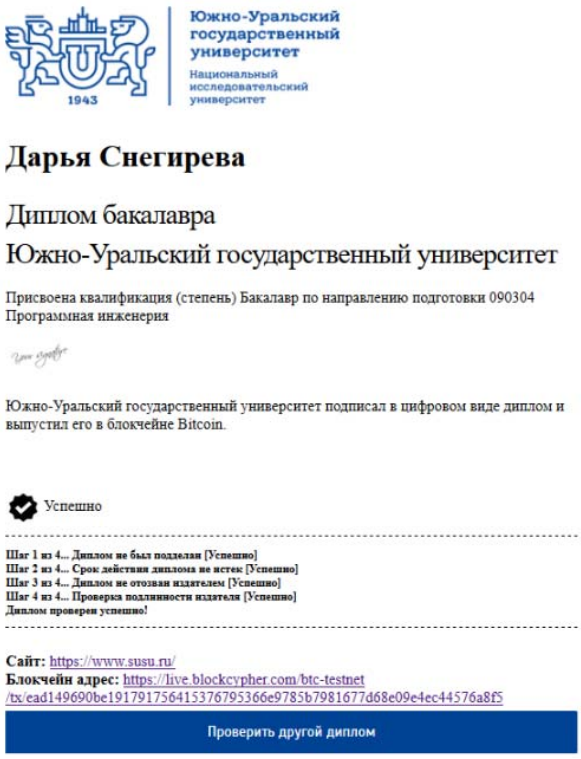

Fig. 9. Test page

VII. CConclusion and Future Work

The article presents the implementation of the issuance and authentication of diplomas using blockchain technology. All source codes are on github in the public domain. Moreover, for the convenience of presenting the results of the system the web service was developed. This system is a prototype of a system that will be implemented on the basis of South Ural State University. For the further work is considered to develop its own blockchain platform.

Acknowledgment

The reported study was funded by RFBR and EISR according to the research project № 19-011-32166.

REFERENCES

[1] Shamsutdinova T.M. Application of the blockchain technology for digital diplomas: problems and prospects // Open Educ. 2019. T. 22. № 6. C. 51–58.

[2] Официальный сайт Финансового университета. [Electronic resource] // URL: http://www.fa.ru/checkdiploma_blockchain/Pages/Home.aspx (date of the application: 29.04.18).

[3] Zhu S., Zhu C., Wang W. A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256 // Entropy. 2018. T. 20. № 9. C. 716.

[4] Mit degree verification. [Electronic resource] // URL: https://credentials.mit.edu/ (date of the application: 29.04.18).

[5] Что такое Блокчейн (Blockchain)? Технология распределенного реестра простыми словами. [Electronic resource] // URL: https://mining-cryptocurrency.ru/blockchain/ (date of the application: 29.04.18).

[6] The Blockchain - Mastering Bitcoin [Book] [Electronic resource] // URL: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch0 7.html (date of the application: 29.04.18).

[7] Who is Vitalik Buterin. [Electronic resource] // URL: https://cointelegraph.com/ethereum-for-beginners/who-is-vitalik-buterin (date of the application: 29.04.18).

[8] «С чем это едят»: что такое блокчейн. [Electronic resource] // URL: https://habr.com/ru/company/bitfury/blog/326340/ (date of the application: 29.04.18).

[9] Тестова, А. «Алгоритмы консенсуса»: Подтверждение доли и доказательство работы. [Electronic resource] // URL: https://habr.com/ru/company/bitfury/blog/327468/ (date of the application: 29.04.18).

[10] OP_RETURN Review. [Electronic resource] // URL: https://cryptolinks.com/998/op-return (date of the application: 29.04.18).

[11] Алгоритмы консенсуса в блокчейне: PoW, PoS, BFT и другие. [Electronic resource] // URL: https://www.bitbetnews.com/novichkam/algoritmy-konsensusa.html (date of the application: 29.04.18).

[12] Камнев, Илья. 3D Блокчейн. Доказательство на лицо. (Po [Electronic resource] // URL: https://habrahabr.ru/post/333708 ((date of the application: 29.04.18).

[13] van Flymen, Daniel. Learn Blockchains by Building One. [Electronic resource] // URL: https://hackernoon.com/learn-blockchains-by-buildingone-117428612f46 (date of the application: 29.04.18).

[14] Декомпозиция blockchain. [Electronic resource] // URL: https:// habrahabr.ru/post/312654/ (date of the application: 29.04.18).

[15] Blockcerts. [Electronic resource] // URL: https://www.blockcerts.org/ (date of the application: 29.04.18).

[16] Документация .NET Framework 4.8. Uri Class. [Electronic resource] // URL: https://docs.microsoft.com/ru-ru/dotnet/api/system.uri?view=netframework-4.8 (date of the application: 29.04.18).

[17] Обозреватель блоков. [Electronic resource] // URL: https://www.blockchain.com/explorer (date of the application: 29.04.18).

[18] A. Averin, N. Zyulyarkina. Mathematical Model of Symmetric Cryptoalgorithm Based on Representing Numbers as Sums of Special Code Elements. 2018 Global Smart Industry Conference (GloSIC). Chelyabinsk, Russia. Volume: 6.